ode 4710-25

DEPARTMENT OF STATE

[Public Notice: 11637]

Privacy Act of 1974; System of Records

ACTION: Notice of a Modified System of Records.

SUMMARY: This system supports the Department of State's Office of the Directorate of Defense Trade Controls'(DDTC) mission of controlling the export and temporary import of defense articles and defense services covered by the United States Munitions List (USML).

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice is effective upon publication, except for the routine uses that are subject to a 30-day period during which interested persons may submit comments to the Department of State. Please submit any comments by March 1st 2022.

ADDRESSES: Questions can be submitted by mail or email or by calling Eric F. Stein, the Senior Agency Official for Privacy, at (202) 485-2051. If by mail, please write to: U.S Department of State; Office of Global Information Systems; A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520. If by email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at Privacy@state.gov. Please write "Munitions Control Records, State-42" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520 or by calling (202) 485-2051.

SUPPLEMENTARY INFORMATION: This notice is being modified to reflect the Department of State's move to cloud storage, an Information Technology (IT)

modernization, and new OMB guidance. The modified system of records notice includes revisions and additions to the following sections: Authority for Maintenance of the System, System Location, Categories of Individuals, Categories of Records in the System, Routine Uses, Storage, and Safeguards. In addition, the Department of State is taking this opportunity to make minor administrative updates to the notice.

SYSTEM NAME AND NUMBER: Munitions Control Records, State-42.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: (a) Department of State domestic data centers located within the United States, with local infrastructure placed overseas at U.S. Embassies, U.S. Consulates General, and U.S. Consulates; and U.S. Missions, (b) within a government cloud platform provided by the Department of State's Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER(S): DDTC Chief Information Officer; 2401 E Street, NW, Washington DC 20037; (202) 663 2023; DDTC-CIO@state.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 22 U.S.C. 2651a (Organization of Department of State); 5 U.S.C. 301 (Departmental Regulations); 22 U.S.C. 2776, 22 U.S.C. 2778, 22 U.S.C. 2779, 22 U.S.C. 2780, and 22 U.S.C. 2751 *et seq.* (Arms Export Control Act); E.O. 13637; International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130.

PURPOSE(S) OF THE SYSTEM: This system enables DDTC to support industry customers as DDTC performs its mission to implement relevant provisions of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) and control the export and temporary import of defense articles and defense services covered by the United States Munitions List (USML).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Exporters of defense articles and defense services with or without Department of State authorization;

applicants for export licenses; registered exporters; brokers for sales of defense articles or defense services who completed registration statements or submitted requests for approval of a brokering activity; and debarred parties. The Privacy Act defines an individual at 5 U.S.C. 552a(a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: Correspondence, registration statements when a principal executive officer or owner is the same as the applicant, and payment for registration fees sent to the Department of State when an individual or business registers as a manufacturer, exporter and/or broker of defense articles or defense services; information on political contributions, gifts, commissions and fees relating to certain sales of defense articles and defense services; license applicants, secondary entity contacts, third-party points of contact, and other relevant entities, may be asked to provide information such as: name, address, nationality/citizenship status, passport/visa/social security number, operator/certificate license, contract and licensing eligibility, contact information (e.g., telephone number, email address), information related to current or past law enforcement charges and convictions, place of birth, financial account numbers, and date of birth; copies of letters to individuals and businesses from the Department of State pertaining to their registration, including notices of suspension and debarment; proposed charging letters and orders and consent agreements pertaining to the Department of State's administrative cases; Federal Register Notices of statutory debarment; correspondence, memoranda, federal court documents, telegrams, other government agency reports, and email messages between the Department of State and other federal agencies regarding law enforcement and intelligence information about defense trade activities pertaining to the subject of the record.

RECORD SOURCE CATEGORIES: These records contain information that is

primarily obtained from the individual, from the organization the individual represents, federal court documents, and intelligence and law enforcement agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Munitions Control Records may be disclosed to:

(a.) Appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(b.) Another Federal agency or Federal entity, when the Department of State determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(c.) The Department of Homeland Security, the Department of Justice (DOJ), the Department of Commerce, and other federal entities, including intelligence and law enforcement agencies to assist in their investigations of violations of the AECA or in the context of multilateral or bilateral export regimes.

(d.) A court, adjudicative body, or administrative body before which the Department is authorized to appear when (i) the Department; (ii) any employee of the Department in his or her official capacity; (iii) any employee of the Department in his or her individual capacity where the U.S. Department of Justice or the Department has agreed to represent the employee; or (iv) the Government of the United States, when the Department determines that litigation is likely to affect the Department, is a party to litigation or has an interest in such litigation, and the use of such records by the Department is deemed to be relevant and necessary to the litigation or administrative proceeding.

(e.) Foreign governments for purposes relating to law enforcement or regulatory matters or in the context of multilateral or bilateral export regimes, in accordance with 22 C.F.R. § 126.10(d)(1).

(f.) Congress to comply with statutory and regulatory reporting requirements in the AECA or ITAR related to certain defense trade transactions.

(g.) Other federal agencies in order to provide independent monitoring of a system of security policy enforcement, malicious activity detection, and security incident response.

(h.) The public, as necessary, to comply with statutory or regulatory requirements or to enable exporters to comply with such requirements, as follows:

i. The periodic publication in the *Federal Register* of names, dates of conviction, and months and years of birth of those on the Debarred Parties List pursuant to the authorities granted in 22 U.S.C. 2778(g), as implemented in 22 C.F.R. § 127.7.

ii. The periodic publication of charging letters, debarment orders, and orders imposing civil penalties and probationary periods in the Public Reading Room of the Department of State, as required by 22 C.F.R. § 128.17, and on the Directorate of Defense Trade Controls website.

iii. The periodic publication of registrant name and address changes on the Directorate of Defense Trade Controls website to assist registrants and applicants in keeping their records current.

The Department of State periodically publishes in the *Federal Register* its Prefatory Statement of Routine Uses. These standard routine uses apply to Munitions Control Records SORN, State-42.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored both in hard copy and on electronic media. A description of standard Department of State policies concerning storage of electronic records is found at https://fam.state.gov/FAM/05FAM/05FAM0440.html. All hard copies of records that contain personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Individual name, company name, DDTC Registration Code, DDTC Case Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records will be maintained in accordance with the Department of State Records Schedule, Chapter 24 Arms Control and International Security Records, Office of Defense Trade Controls (A-24-048-01a(1)) **,** as approved by the National Archives and Records Administration (NARA) and outlined at https://foia.state.gov/Learn/RecordsDisposition.aspx.

More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N. W., Room B-226; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department of State OpenNet network users are required to take the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before a user is granted access to Munitions Control Records, they must first be granted access to the Department of State computer network.

Department of State employees and contractors may remotely access this system of records using non-Department of State owned information technology. Such access is subject to approval by the Department of State's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department of State's information system is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a thorough background security investigation. Access to the Department of State, its annexes and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized files is password-protected and under the direct supervision of the system manager. The

system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Information that conforms with Department of State-specific definitions for Federal Information Security Modernization Act (FISMA) low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department of State's Cloud Program Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department of State policy, systems that process more sensitive information will require more stringent controls and review by Department of State cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology's (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department of State data center by the Department of State key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will

additionally be subject to continual auditing and monitoring, multifactor authentication mechanism utilizing Public Key Infrastructure (PKI) and NIST 800 53 controls concerning virtualization, servers, storage and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or to amend records that pertain to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N. W., Room B-226; Washington, DC 20520. The individual must specify in the written correspondence that he or she wishes the Munitions Control Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury that the information in the written is true and correct; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Munitions Control Records include records that pertain to the individual. Detailed instructions on Department of State procedures to access and amend records can be found at the Department of State's FOIA website at https://foia.state.gov/Request/Guide.aspx.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest records should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N. W., Room B-226; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N. W., Room B-226; Washington, DC 20520. The

individual must specify in the written correspondence that he/she wishes the Munitions Control Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury that the information contained in the written correspondence is true and correct; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Munitions Control Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), portions of certain records contained within this system of records are exempted from 5 U.S.C. 552a (c)(3),(d),(e)(1),(3)(4)(G),(H) and (I), and (f). See 22 CFR 171.26.

HISTORY: Previously published at Public Notice 6140 State-42, System Name: Munitions Control Records. Volume 73, Number 55; March 20, 2008.

Eric F. Stein,

Deputy Assistant Secretary,

Bureau of Administration,

Global Information Services,

US Department of State.

[FR Doc. 2022-02202 Filed: 2/2/2022 8:45 am; Publication Date: 2/3/2022]